

REPORT DOCUMENTATION PAGE**Form Approved**
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Service, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 29-04-2011		2. REPORT TYPE Master of Military Studies Research Paper		3. DATES COVERED (From - To) September 2010 - April 2011	
4. TITLE AND SUBTITLE Cybersecurity: The Next Threat to National Security				5a. CONTRACT NUMBER N/A	
				5b. GRANT NUMBER N/A	
				5c. PROGRAM ELEMENT NUMBER N/A	
6. AUTHOR(S) LCDR Jonathan W. Sims, USN				5d. PROJECT NUMBER N/A	
				5e. TASK NUMBER N/A	
				5f. WORK UNIT NUMBER N/A	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				10. SPONSOR/MONITOR'S ACRONYM(S) N/A	
				11. SPONSORING/MONITORING AGENCY REPORT NUMBER N/A	
12. DISTRIBUTION AVAILABILITY STATEMENT Unlimited					
13. SUPPLEMENTARY NOTES N/A					
14. ABSTRACT The Information Age has given birth to a new cyber domain that has minimized essential barriers and increased cross border partnerships while augmenting adversaries. Governments are responsible for protecting national security and public welfare. The nation will have to establish laws that address cyber-threats and hold persecutors of cyber attacks accountable; develop regulations requiring security in certain sectors; establish organizations and programs that help with cybersecurity; and allocate money for cyber-public awareness, defense research, and education. Although the federal government currently executes efforts toward developing cyberspace governance and security, these policies and initiatives are limited in delivering an effective national cybersecurity strategy.					
15. SUBJECT TERMS asymmetric, computer network defense, cyber domain, Cyber Storm, cyber warfare, cybersecurity, cyberspace, fifth domain, Industrial Age, Information Age, Internet, OODA Loop, network security					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 36	19a. NAME OF RESPONSIBLE PERSON Marine Corps University / Command and Staff College
a. REPORT Unclass	b. ABSTRACT Unclass	c. THIS PAGE Unclass			19b. TELEPHONE NUMBER (include area code) (703) 794-3330 (Admin Office)

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, VA 22134-5068*

MASTER OF MILITARY STUDIES

TITLE:

CYBERSECURITY: THE NEXT THREAT TO NATIONAL SECURITY

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

Jonathan W. Sims
LCDR USN

AY 10-11

Mentor and Oral Defense Committee Member: Dr. Paul D. Goss

Approved: [Signature]

Date: 29 April 2011

Oral Defense Committee Member: Dr. Douglas E. Stencel

Approved: [Signature]

Date: 29 April 2011

Executive Summary

Title: Cybersecurity: The Next Threat to National Security

Author: Lieutenant Commander Jonathan W. Sims, United States Navy

Thesis: The United States lacks a comprehensive national strategy that effectively addresses cybersecurity. Cybersecurity can no longer be an esoteric concept understood by few; it must be addressed and understood by all public-private sectors and international activities. In order to meet this critical need, the United States must employ a dynamic decision-making process that utilizes Boyd's OODA Loop concept. Engaging this sound strategy would enable the United States to adapt to the unpredictable and rapidly changing cyber environment.

Discussion: The Information Age has given birth to a new cyber domain that has minimized essential barriers and increased cross border partnerships while augmenting adversaries. Governments are responsible for protecting national security and public welfare. The nation will have to establish laws that address cyber-threats and hold persecutors of cyber attacks accountable; develop regulations requiring security in certain sectors; establish organizations and programs that help with cybersecurity; and allocate money for cyber-public awareness, defense research, and education. Although the federal government currently executes efforts toward developing cyberspace governance and security, these policies and initiatives are limited in delivering an effective national cybersecurity strategy.

Conclusion: The United States has been successful at conducting cybersecurity at the tactical level; however, the federal government must focus on establishing a comprehensive strategy that clearly articulates roles and responsibilities of organizations, and effective timelines. The pervasive and rapidly evolving cyber threats must be countered with forward-thinking, adaptable solutions, and effective partnerships.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

Executive Summary	i
Disclaimer	ii
Table of Contents	iii
Preface	iv
Introduction	1
Orientation of the Cyber Environment.....	1
Cyberspace (The Fifth Domain)	2
The Cyber Attacker (The Human Element)	3
Motives and Goals	4
Modernized Cybersecurity Strategic Framework	6
Observation	8
Orientation	8
Decision	9
Action.....	9
Interoperability and Agility	10
Orientation Case Studies	13
Estonia: Web War I.....	13
North Korea: Fourth of July.....	15
Operation Buckshot Yankee: Remove Drives in a Flash.....	16
Case Study Analysis.....	17
Implications for the United States Cybersecurity Strategy	19
Conclusion.....	24
Bibliography.....	25
Notes.....	28

Preface

Eight years ago I had the gracious opportunity of being selected into the newly formed United States Navy Information Professional (IP) community. In this role, I personally experienced the nation's ongoing challenge within the cyber domain infrastructure by observing, accessing and mitigating cyber threats across military services, government agencies, and private sectors. It is this experience that directly engaged my interest in researching methods to strategically address the growing cyber threat. The goal of this project is to demonstrate the importance of implementing a dynamic cybersecurity strategic framework that would properly address the continuously growing cyber threat in the Information Age. Furthermore, demonstrate and evaluate evidence supporting the critical need for the United States to remove itself from the antiquated dogma of the Industrial Age and realign itself with the rapidly changing Information Age.

I would like to acknowledge Dr. Paul Gelpi for providing expert recommendations and essential technical assistance. Additionally, I would like to thank Lieutenant Colonel Loretta Vandenberg, United States Marines Corps for offering sound guidance and critical feedback. Finally, I would like to thank my wife, Deborah, for encouraging and supporting me during this exciting venture.

Introduction

Cyberspace has become the cornerstone of United States communication, commerce, military command and control, emergency services, mass transit, power plant distribution, and numerous other critical infrastructures essential to enabling and sustaining twenty-first century society. Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers.¹ As societal dependency on information technology grows, so do cyber threats. A diverse group of nation-states, non-state actors, state-sponsored groups, and individuals may wage malicious cyber attacks on a target. Cyber and sabotage attacks on critical United States economic, energy, and transportation infrastructures may be viewed by invested adversaries as a way to circumvent United States strengths on the battlefield and attack United States interests directly at home.² In support of the national security strategy, the nation must institute a multilateral strategic framework that focuses on the dynamic challenges of cyber in the Information Age.

Orientation of the Cyber Environment

The driving force behind cybersecurity is the threat of cyber attacks. Each level of a cyber-physical infrastructure, comprised of operational software, information, and people - is susceptible to security breakdown, whether through attack, infiltration, or accident. Cyber threats are asymmetric because they allow the few to perpetrate attacks upon the masses. Through an Internet-connected computer, a belligerent cyber actor may conduct a cyber attack with minimal technical and operational resources. With a minimal chance of failure, cyber attacks offer a high return for a low financial investment. Because of the permeable nature of sophisticated networks, a cyber actor may infiltrate an adversary's network with minimal risk of

discovery. Asymmetric attributes provide a cyber attacker with limited conventional warfare capability the means to challenge the United States directly and negate U.S. military superiority. The increasing trend of ubiquitous computing with cyber-threats is characterized by an attacker, a target system, a set of actions against the target, and the consequences resulting from the attack. Consequences include damages to the target, direct and indirect losses to victims, and variable impact on third parties. As cyberspace becomes increasingly pervasive and entrenched in society, it spawns the availability of more targets to attack, and an increase in the population of skilled attackers. Defenders must familiarize themselves with the environment by understanding not only the cyber domain but also the human element, the attacker, their motives and goals. Consideration of the identified key components will provide greater fidelity to the orientation phase of the decision-making process.

Cyberspace (The Fifth Domain)

Physical space is the dimension most often associated with security. Physical space whether land, sea, or atmosphere, is demarcated into territories under the jurisdiction of sovereign state law. Throughout history, armies have been deployed across territories and bodies of water—whether they were provinces, kingdoms, countries, or whole empires—in order to defend their own land or lay claim to other lands (in the name of security or national aggrandizement).³ Conversely, cyberspace is unconfined to a spatial dimension or effectively sanctioned by sovereign states or international law.

Globally interconnected, cyberspace is a realm of digital information and communication that consists of decentralized computer networks with no single authority to supervise or regulate operation. In the past several years, cybersecurity has transitioned from an esoteric concept only comprehended by computer scientists and information system managers to a major national

security threat requiring the attention of the public and policy makers. President Barack Obama has declared America's digital infrastructure to be a "strategic national asset."⁴ Through the course of developing national policies and strategies, cyberspace has become the fifth domain of warfare, after land, sea, air, and space.

Cyberspace is a realm that is constantly growing worldwide and unlike the conventional domains, it cannot be rigidly demarcated into national boundaries or other territorial units. Because of this idiosyncrasy, *The National Strategy to Secure Cyberspace* has emphasized that securing cyberspace is a global matter due to the interconnectedness of the world's computer systems. Conventional based policies, strategies, and initiatives from years past do not directly address the new challenges and issues independently unique to the cyberspace domain, nor do they completely coincide with the legislation and agenda of foreign nation-states. Securing global cyberspace will require international cooperation to raise awareness, share information, promote security standards, and investigate and prosecute cybercrime.⁵

The Cyber Attacker (The Human Element)

Technology is normally associated with cybersecurity; however the human element cannot be disvalued or ignored. United States Air Force colonel John Boyd argued that "Machines don't fight wars...Humans fight wars."⁶ A cyber threat is always given its existence from a human element. A wide spectrum of malicious cyber attackers exists from individual hackers, to criminal enterprises, to terrorist groups, to corporations, to nation-states. Fundamentally, each attacker can be classified of two types, a sovereign state or non-state actor. A non-state actor whose purposes are criminal and who is subject to the jurisdiction of one or more sovereign states includes hackers, criminal enterprises, terrorist groups, and corporations. Terrorists constitute a more serious set of non-state actors and are of concern both to law enforcement

agencies and national security agencies.⁷ Considered the most serious, nation-states have the means and resources to employ cyber-weapons that can augment or replace the conventional kinetic ones. According to some analysts, as many as twenty countries have cyber-warfare capabilities, including China, Russia and North Korea.⁸ Belligerent state actors normally target other sovereign states, although specific targets may be identical to those of non-state attackers. Unfortunately, these actors are not mutually exclusive and could amalgamate and create a customized threat. The attackers do not need to amass great arms, it can all be done covertly and cheaply, by hiring outside expertise.⁹

Motives and Goals

In general, an active or high-profile cyber attacker will have a motive and goal to attack a target. Goals and motives have separate definitions. However, they are interrelated when attacking a target. Motives are human objectives, while goals are technical or tactical objectives. A motive for an attacker would be to conduct espionage, obtain monetary gains, and inflict malicious harm or further national or ideological interests. When a cyber attacker acts based upon a motive, at least one of the following three goals are attempted:

Goal 1: Attacker attempts to damage or curtail the effectiveness of critical cybersecurity infrastructure components. Attacks generally cause one or more critical components of an infrastructure to either become inoperable or operate below capacity. Examples include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. To mount such an attack, the attacker secures access to a number of unprotected computers and instructs them to send a large number of messages to the target website, either requesting information and hence saturating the target's input capacity, or transmitting invalid information that causes the target

site to crash.¹⁰ Based on the level of the attack and infrastructure impacted, the attack could severely impair operations on the national security level.

Goal 2: Attacker attempts to gain unauthorized access to the target's sensitive information. Corporations, universities, state and local governments, and other organizations have become critically dependent upon their information infrastructure containing mission critical information, including product data, trade secrets, client records, and personnel information. Executed with worms and viruses, this attack can create a trapdoor that can allow an unauthorized entry into a network or into the software program. Often after an initial entry, a cyber criminal or cyber warrior leaves behind a trapdoor to permit future access to be faster and easier.¹¹ An actor may benefit financially by selling this confidential information to anyone that is interested such as the target's competitor or adversary. The actor cannot only use or sell the sensitive information they extracted from the target system, but also modify or delete the information causing detrimental effects on the target system.

Goal 3: Attacker attempts to gain unauthorized access to cyber resources for exploitation. An actor conducts scans generated by automated tools and malware, looking for vulnerable ports with nefarious intent.¹² Consequently, these ports could be associated with critical Distributed Control Systems (DCS) or Supervisory Control and Data Acquisition (SCADA) systems. SCADA and DCS systems typically monitor and control industrial-based infrastructures such as water treatment facilities, communication systems, utility companies, nuclear powerplants, and various industrial processes. A compromised SCADA or DCS system can result in financial losses, property and environmental damage, personal injury, or death.¹³

To accomplish the final goal, a cyber attacker may have to conduct infiltration in phases or combine the goals mentioned above. For example, the cyber attacker's motive may be to

conduct espionage against a target's cyber network and sell the confidential information. The attacker attempts to gain unauthorized access to the target's network by conducting an automated scan of open ports via malware that was surreptitiously loaded by a malicious e-mail attachment (Goal 3). Once the attacker has identified the open or unguarded ports, a distributed denial of service attack is performed and the protective infrastructure is paralyzed (Goal 1). The attacker gains access to the targets network and obtains the sensitive information and sells it to the highest bidder (Goal 2).

Understanding the cyber environment allows defenders to properly assess the situation and make coherent decisions. This information will be used within the modernized strategic framework for cybersecurity. Defenders must familiarize themselves with the environment by understanding the cyber domain, the human element the attacker, and the motives and goals. Understanding these key components will provide greater validity to the orientation phase of the decision-making process.

Modernized Cybersecurity Strategic Framework

The Nation's cybersecurity strategy must adapt to the rapidly changing circumstances of the cyber environment and maintain cohesion across the overall effort. With cyber protection the government must confront a multiplicity of issues, ranging from private-public interface, security, human capital, research and development, and governance to others such as the implications of the increased volume of traffic, the potential move from IPv.4 to IPv.6, net neutrality, and the nature of the United States global role.¹⁴ Several decades ago a United States Air Force colonel and military strategist, John Boyd, developed a decision-making model called the Observation-Oriented-Decision-Action (OODA) Loop. Boyd's concept created the ability to formulate and implement strategies in constantly changing environments. Boyd based his

decision-making model on the Blitzkrieg method that allowed Germany in World War II to “conquer an entire region in the quickest possible time by gaining initial surprise and exploiting the fast tempo/fluidity-of-action ... as basis to repeatedly penetrate, splinter, envelop, and roll-up/wipe-out disconnected remnants of [the] adversary organism.”¹⁵ The OODA Loop is a cyclic process that adapts from the continuous feedback obtained from each phase of its open system. The purpose of the OODA Loop is for an opponent to process through the decision cycle expeditiously, observing, and reacting to the changing environment more quickly than its adversary. In effect, the prevailing opponent moves “inside the adversary’s OODA Loop” by rapidly altering the environment or compressing time to a point the adversary is cannot reach the accelerated tempo and the relevance of its OODA Loop becomes obsolete. However, the victor cannot become complacent and must continuously proceed to the next decision cycle to sustain its success. In the past decades, the OODA Loop’s adaptability in a rapidly changing environment has become an important decision-making model in the public and private sectors. The nation can apply this same decision-making model to computer network operations (CNO) and computer network defense (CND). An example of Boyd’s OODA Loop incorporated within the Cybersecurity Strategy Formulation Model is introduced in Figure 1. Decomposition of the OODA Loop model illustrates its relevance in formulating and implementing cybersecurity strategies.

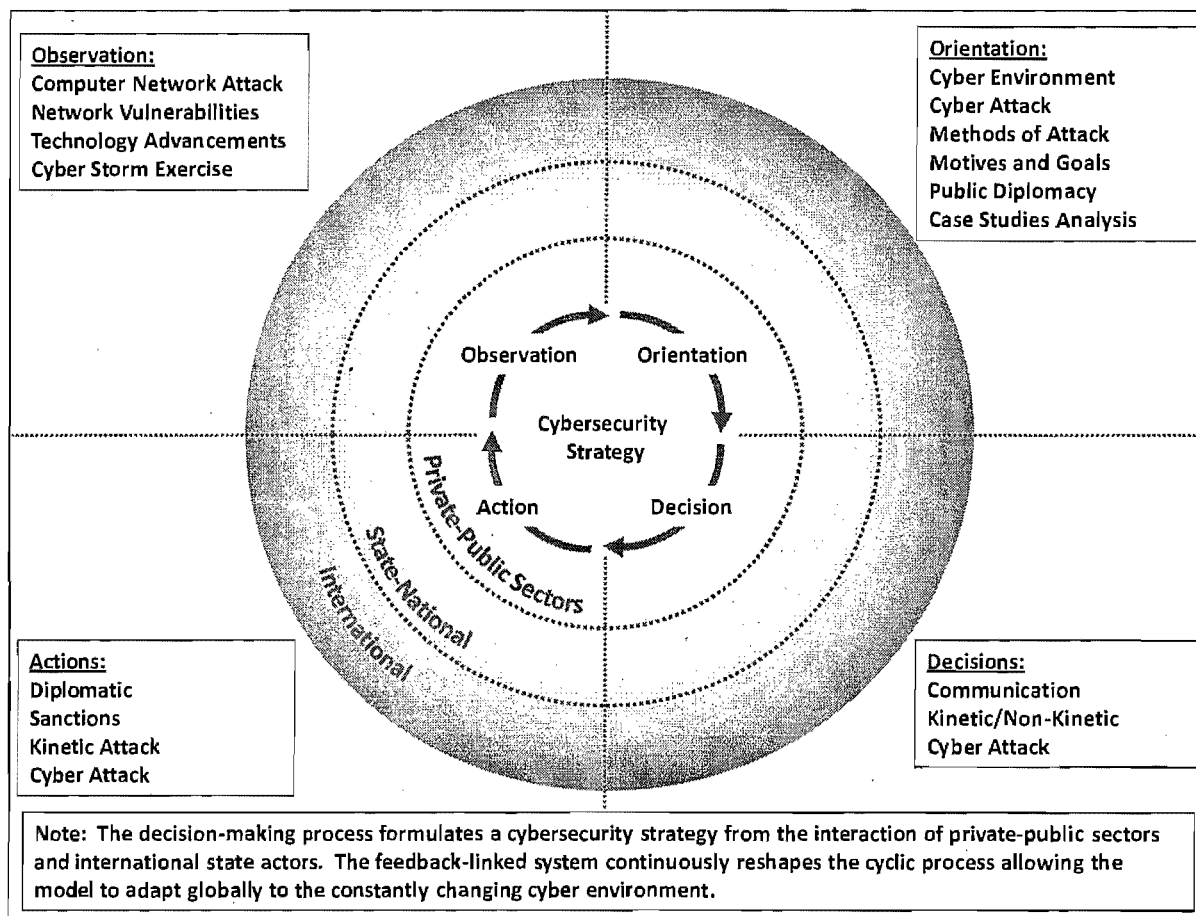


Figure 1. Boyd's OODA Loop incorporated within the Cybersecurity Strategy Formulation Model

Observation

The observation phase is the earliest stage of the OODA Loop process that provides real-time raw data. This phase continuously collects data as the circumstances unfold. This phase can directly be applied to computer network systems actively monitoring for anomalies, malicious attacks, system vulnerabilities, and intrusions. The collected data is forward-feed to the orientation phase for compilation.

Orientation

When formulating strategy the most critical phase in the decision-making model is "Orientation." Orientation strengthens the epistemic power of the OODA Loop. The raw data

obtained from the observation phase is analyzed and synthesized into usable information that can be used in the decision phase. The orientation phase is a “nonlinear feedback system” that spontaneously generates a new cognitive image of the unfolding circumstances.¹⁶ This cognitive tapestry of images is forward fed to the decision phase of the OODA Loop process.

Decision

The situational awareness gained from the orientation phase can be used to formulate possible courses of action, determine acceptable risk, hypothesize possible outcomes, and make critical selections. Moreover, the strategic decision-making can be enhanced from experience, training, case studies assessments, and innate ability. For cybersecurity this can be used to establish legislation and policies relevant and succinct to the current cyber environment.

Action

Predicated upon opportunities discovered in the decision phase, the action phase executes the strategy. Once the action is executed, the OODA loop closes. As a result, the OODA Loop spontaneously reopens with the changed environment affected by the action taken. The decision-making model must continue the whirl of reorientation, mismatches, analysis/synthesis over and over again ad infinitum.¹⁷ Within the action phase, strategic guidance germane to the current cyber environment is provided to the subordinate organizations. Boyd emphasized that “the commander is able to maintain a high operational tempo and rapidly exploit opportunity because he makes sure his subordinates know his intent.”¹⁸

The strategy formulation model also illustrates the overlapping spheres of influence from the private-public sector and international state actors. Feedback obtained from interaction of the phases and echelons constantly reshape the cyclic process, allowing the model to adapt globally to the cyber environment. In order for the model to formulate a cybersecurity strategy germane

to the current cyber threat, emphasis must be placed on the orientation phase of the process. This phase develops the epistemic foundation of the cybersecurity strategy. The orientation phase is a shaping function that provides dimensionality, adaptive context, and validation to the cyber phenomena. Becoming oriented to a competitive situation means bringing to bear the cultural traditions, genetic heritage, new information, previous experiences, and analysis/synthesis process of the entity doing the orienting.¹⁹

Interoperability and Agility

In order to overcome the cyber threat in the Information Age, the United States' strategic framework must ensure enhanced interoperability and agility within the joint enterprise architecture that involves coercive movement between the nation, private-public sectors, and international activities. Most of the existing philosophy, doctrine, and practice of command and control were developed and perfected during (and thus reflect) the Industrial Age.²⁰ Industrial Age organizations have evolved into multi-layered hierarchies populated with stove-piped organizations and independent efforts. A typical Industrial Age strategic framework is shown in Figure 2. Each entity in the framework operates in a closed loop system with limited communication with external entities. The components in the framework are almost mutually exclusive from one another. With its limited agility and interoperability, this organic framework is not effective in handling a dynamic cyber threat. The framework also illustrates the varying tempos between the private-public sectors, nation-state, and international activities. These tempos are based on the current level of effectiveness within the organizations. The legislation, which should be the foundation for this strategic framework, is antiquated and not germane to the cyber domain. In addition, the Industrial Age legislation is permeable, allowing an attacker to

circumvent the system by claiming plausible deniability and finding places of refuge not address in the legislation.

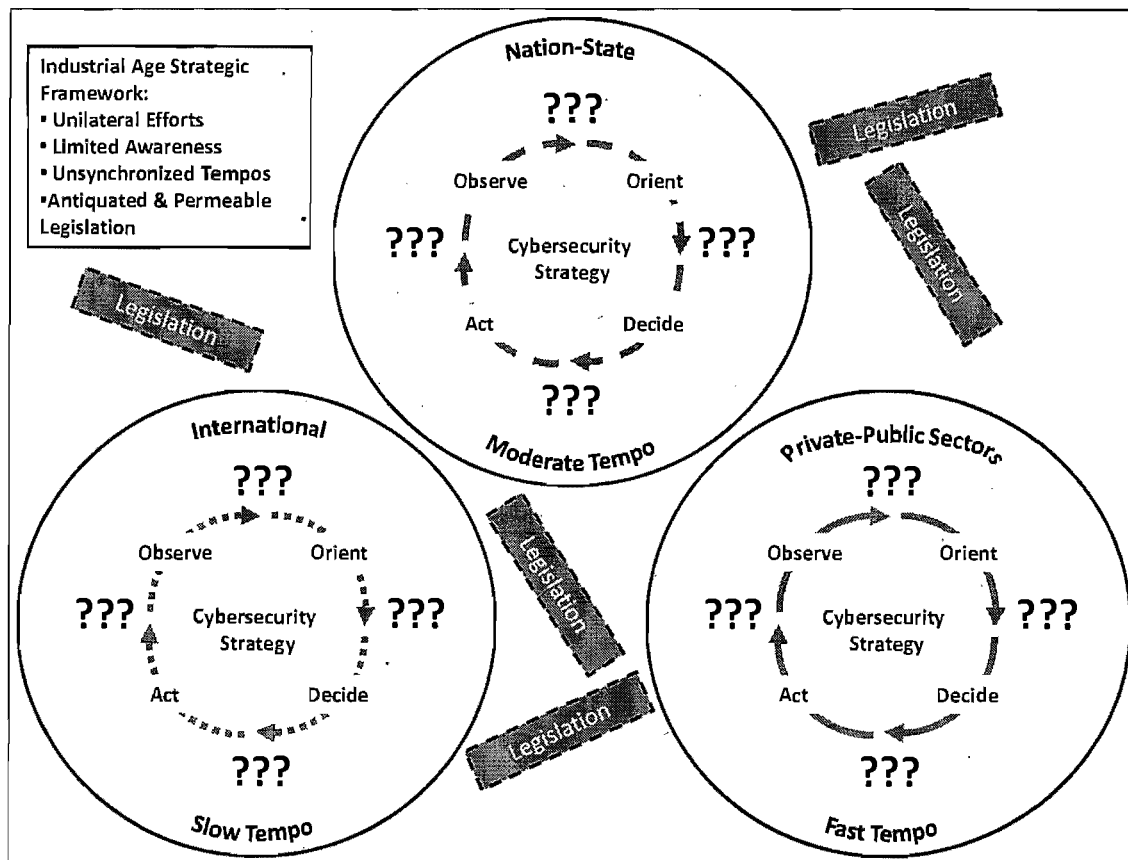


Figure 2. Failing cybersecurity strategy with antiquated legislation

An effective strategic framework for the Information Age would include a decision-making process that uses both organic and inorganic assets to formulate a strategy that is germane to current cyber environment as seen in Figure 3. In order to reduce permeability, it is imperative that the Nation and its partners impose legislation reform for the Information Age. This reformed legislation would create a solid foundation or basis for the Cybersecurity Strategy Formulation Model. The cybersecurity strategy model also encourages interaction and continuous feedback with all entities in the model. This consolidated effort improves the agility and interoperability within the cybersecurity strategic model. The Strategic International Cyber

Council presented in the model is a hypothetical authority that is involved in establishing the conditions and the overall intent for the participating entities. Command in the Information Age is ultimately not the sole responsibility of any single individual. It is a shared and distributed responsibility.²¹

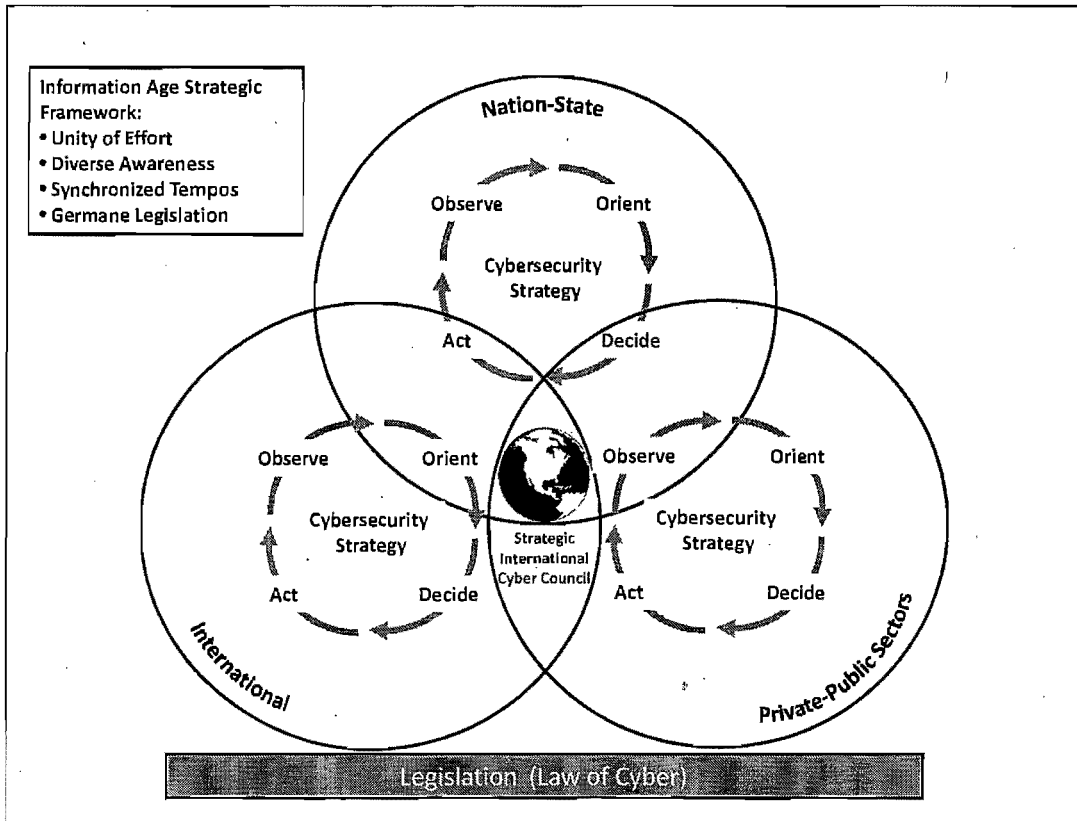


Figure 3. Effective cybersecurity strategy with legislation germane to cyber

The following case studies demonstrate not only the strategic and legislative challenges being faced by the organizational activities but also demonstrate the importance of having a framework that has components that are integrated with one another. Furthermore, a greater understanding will be provided on the importance of having a legislation system specific to cyber. Establishing this system is not something that can be accomplished overnight, activities must invest time and effort to reach this optimum level of transparency in order to be effective in the Information Age.

Orientation Case Studies

The following three case studies will demonstrate the challenges state actors face when confronted with a tenacious cyber threat. Although the selected case studies are geographically dispersed outside the boundaries of the United States, they provide a relevant rational of a state's susceptibility to a cyber threat. Cyberspace is boundless and does not abide to conventional geographical demarcations. Hence, a ubiquitous cyber attack experienced in Estonia or South Korea can also have a transverse impact in the United States. The attack can be initiated from an unexpected actor like North Korea or Afghanistan, who may not appear to have the prowess to carry out technologically advanced attacks. The case studies provided will serve as a premise of how a dynamic decision-making process can be used to formulate strategy for the constantly evolving cyber domain.

Estonia: Web War I

In April 2007, Estonia made a controversial decision to move a Soviet war memorial from its capital center in Tallinn to a less prestigious location. Russians see the monument as a sacred memorial to the millions of Soviet soldiers who died in [World War II], while to Estonians it is a reminder of 50 years of Soviet occupation.²² The removal of the memorial caused protests and riots and intensified a row between Russia and Estonia. Estonia soon became the victim of malicious cyber attacks. Ranking higher than the United States, Estonia along with South Korea had become the most digitally connected nation in the world. Conversely, the country's advancements in broadband connectivity and utilization of highly integrated systems and applications within the cyber domain made Estonia the perfect target for a cyber attack.

The first wave of cyber attacks began at 10 p.m. on April 26, the day the decision was made to move the Soviet war memorial. Prior to the attack, Estonian technical experts set up extra computer servers, prepared and erected firewalls around government websites, and placed extra staff on duty. The first wave of cyber-attacks against official websites fizzled out after Estonian Foreign Minister Urmas Paet publicly declared that many of the attacks had originated from Russian government computers.²³ Unfortunately, Estonia's effective defense strategy was short lived and a massive wave of cyber attacks began to infiltrate the country's cyberspace.

On April 30, 2007, the second wave of attacks began from around the world. Estonian Websites were defaced with Russian propaganda. Hackers broke into the website of the Reform Party, posting a fake letter of apology from the prime minister, Andrus Ansip, for ordering the removal of the highly symbolic statue.²⁴ Servers supporting the most used websites in Estonia were bombarded with a series of cyber access requests, choking the servers and routers. These distributed denial of service attacks were implemented through the use of *botnets*, a network of computer systems surreptitiously usurped by hackers through malicious software (e.g. Trojans and worms), and banded together like an army of soldiers or "zombies" sending distributed denial of service attacks to attacker's targets of interest. As a result, Estonians were left unable to use websites of government ministries, banks, newspapers, or pertinent online services. Internet security experts rushed from Europe and North America to provide assistance to Estonia. Estonia also brought the matter before the North Atlantic Council of the North Atlantic Treaty Organization (NATO). An ad hoc response team was assembled and they began trying countermeasures and tracing the origins of the cyber attack.

The third wave of attacks commenced again on May 9. Traffic across the country's cyber network activity spiked to thousands of times the normal throughput due to the elaborate *botnet*

attack. "May 10 was heavier still, forcing Estonia's biggest bank to shut down its online service for more than an hour. Even now, the bank Hansapank, is under assault and continues to block access to 300 suspect Internet addresses. It has had losses of at least \$1 million."²⁵ The attacks eventual subsided on May 10 when the leases for the *botnet* routers expired. The Russian Government claimed that the cyber attacks were a populist response that was beyond the control of the Kremlin.²⁶ Following the cyber attack, NATO established the cyber defense center in Tallinn. The media heralds consider the Estonian incident as the first public nation-state conflict in cyberspace and thus labeled it Web War I (WWI).

North Korea: Fourth of July

In June 2009, the United States publically announced that it would be conducting another cyber war exercise known as Cyber Storm. Since 2006, Cyber Storm had been conducted every two years to test the defense of computer networks. The exercise challenged players to identify policies and procedures required for sharing information with groups internal and external to their organizations, such as across Federal and State departments, private organizations, and across international borders.²⁷ South Korea and Japan were members of the international community that participated in the exercise. During the time of the announcement, North Korea was actively conducting ballistic and nuclear weapons tests in violation of United Nations Security Council resolutions. Hence, North Korea believed that Cyber Storm was an attack against them in retaliation.

On July 4, North Korea began shooting short-range ballistic missiles into waters off its east coast. Subsequently, a massive cyber attack was paralyzing websites in the United States and South Korea. Initially affected, were 40,000 computers around the world compromised by a *botnet* virus, acting as an army of zombie computers. The zombie computers were instructed to

continuously ping a list of United States and South Korean government websites and international companies in another distributed denial of service attack.

Similar to Estonia, a second wave of cyber *botnet* attacks infected another 30,000 to 60,000 computers. At this time, the focus was on the South Korean cyber domain, affecting government organizations, vaccine firms, financial institutions, and Web portals. The attackers were apparently convinced that the attacks on United States sites were no longer going to be effective after the government and major corporations began working with Internet service providers (ISPs) to filter out the attacks.²⁸

At 1800 hours on 10 July 2009, the final wave began. Approximately 166,000 computers across seventy-four countries were bombarding the sites in South Korea focusing on the same targets as the second wave. Fortunately, the attack did not try to gain control of any government system or essential service. Eventually the attacks subsided and the damage was contained. It was later discovered that the army of zombie computers were sending information to eight command and control servers. Ironically, the eight command and control servers were in South Korea, the United States, Germany, Austria, and the country of Georgia. Further investigation by the Bach Khoa Internetwork Security (BKIS) revealed that the eight servers were being controlled by a server in the United Kingdom. However, it was later discovered that the server in the United Kingdom was being controlled by a server in Miami, Florida, via a “virtual private network (VPN), which made it appear as though the master server was in Britain instead of in the United States.”²⁹

Operation Buckshot Yankee: Remove Drives in a Flash

In 2008, the United States faced the most significant breach in its military information system network. A foreign intelligence agent intentionally placed an infected memory flash

drive into a U.S. military computer. The flash drive contained a virus called “Agent.btz,” a variation of the “SillyFDC” worm, which spreads by copying itself to thumb drives and the like.³⁰ When the infected drive or disk is placed into another computer it replicates itself again on the computer. The virus creates backdoors across the network and allows code to be downloaded from foreign remote command and control servers. The code spread undetected on both Non-classified Internet Protocol Router Networks (NIPRNet) and Secret Internet Protocol Router Networks (SIPRNet). The virus had the potential to infect more than 15,000 networks and 7 million computing devices across dozens of countries within the U.S. military’s cyber domain.

The incident was deemed classified and the Department of Defense commenced Operation Buckshot Yankee to counter the virus attack. Service members and government employees were directed to cease use of all Universal Serial Bus (USB) storage media devices, which included flash drives and personal portable hard drives. The government security team conducted routine scans across the networks to ensure personnel were adhering to the USB ban. The operation engaged the Pentagon in a 14-month battle to mitigate the vulnerability. The Pentagon never disclosed how many computers were compromised or how much classified information was lost. However, the tortuous endeavor caused the military to expeditiously standup U.S. Cyber Command, which was assigned the responsibility of defending the Department of Defense information networks.

Case Study Analysis

The attacks in Estonia, South Korea and the United States provide orientation to the ongoing challenges faced today in defending against an unpredictable cyber threat. The most critical aspect of the aforementioned case studies is the limitation of authority across international

borders. When conducting an asymmetric cyber assault the attacker has the advantage. The attacker has the opportunity to conduct the attack at their proposed time and place, while the defender is forced to safeguard the entire network without interruption. The attack could arrive in any scale, novelty, scope or complexity. Provided with the anonymity of cyberspace, the attacker can conceal their physical location and deny responsibility for the attack. If North Korea hypothetically did not have the prowess to conduct the cyber attack against the United States or South Korea, they had the means to enlist the help from an outside source, such as China or a criminal organization. If the offender were identified in China or North Korea, is there legislation to prosecute or retaliate against the offender?

The United States' laws directed for cyberspace are decades old and were intended for technologies prior to the cyber-centric era. Furthermore, these laws were of a domestic nature and only applicable to the United States. While many facets of the traditional law of armed conflict paradigm do apply, there are also aspects that do not and that are inadequate in either deterring hostile acts or in containing the potential escalation that could result from cyber attacks.³¹ Domestic criminal law, law of armed conflict, and international law does not properly deter states or non-state actors from using cyber attacks to pursue motives that are detrimental to the national security of the United States. President Obama's *Cyberspace Policy Review* concluded that the United States needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force.³² Legislation must be broad enough to account for emerging technology, while tailored to take advantage of current strengths of the agencies that will be responsible for its the execution and enforcement. Like the international body of law concerning

justification to engage in war (*jus ad bellum*) and the limits to acceptable wartime conduct (*jus in bello*), there needs to be a public international body of law specific to cybersecurity. This body of law would allow authorities to prosecute and combat cyber attackers across the globe, possibly deterring future attackers. To develop an effective strategy, the nations must develop policies and legislation that adapt to the rapidly evolving cyber environment.

Currently, there is limited legislation that crosses international borders that directly addresses cybersecurity. The attacker, even if discovered, is often protected by legal ambiguities and inconsistencies with varying state legal systems. Moreover, public international law does not have an established compulsory penal system for offenders. Through an “ad hoc” system, alleged offenders are assigned to a particular state for prosecution. The state’s handling of the prosecution may not be in consensus with the international community. The Cybersecurity Strategy Formulation Model would provide a medium for an integrated international effort and establish a consensus of legislative initiatives. Legislative initiatives intended to improve cybersecurity have been presented in recent years to address cyber threats. However, these initiatives have been challenged by a number of issues, including questionable geographic locations of attackers, limited lexicons specific to cyber, and the increasing number of sophisticated threats producing new vulnerabilities on the nation’s information framework. The legislative framework for cyber needs to be restructured with national and international involvement and constitute a dynamic decision-making process that will create laws that are transversal from state to state and germane to the cyber offenses.

Implications for the United States Cybersecurity Strategy

As presented in the case studies, the United States has succeeded in countering numerous cyber attacks at the tactical level. However, America has handled cyber threats in a typical

bureaucratic fashion inherent from the Industrial Age. This method of operation has proven to be antiquated and irrelevant at defending against the rapidly evolving cyber threat in the Information Age. Tactically treating the “symptoms” of a cyber attack without a decisive strategy is not sufficient. The government must field a cure that will apprehend the attacker, the “disease,” and enforce punitive measures upheld by domestic and international legislation. Cybersecurity can no longer be an esoteric concept understood by few and handled autonomously. The nation’s policymakers and defenders must take prudent measures at strategically identifying policies requiring groups to share information internally and externally of their organizations, such as across public and private organizations, Federal and State departments, and across international borders. Information and communication networks are primarily owned and operated by the private sector, both nationally and internationally. Hence, cybersecurity will require a partnership with local, state, and federal government agencies, private sector, and international support from the nation’s allies.

The International community must continue to support contingency exercises, like Cyber Storm. Cyber Storm tests government and private sector communications, procedures, and policies in response to diverse cyber attacks and identify where additional planning and process enhancements are required. Participants include private sector, federal, state, international governments, including Australia, Canada, New Zealand, and the United Kingdom. Cyber Storm greatly strengthens the nation’s cybersecurity preparedness and response mechanisms by applying lessons learned from the exercises. This exercise can continue to be valuable tool for developing a comprehensive security policy. However, this exercise is only a starting point that could be adapted into the observation phase. The rapid changing cyber environment needs a

routine process that continuously adapts. An exercise conducted every 1-2 years is not sufficient enough for the orientation of the of the cyber domain.

In early 2000, officials recognized that cyber threats became more pervasive and catastrophic threatening the national security of the United States. The legislative and executive branches of government took leading roles in formulating a cybersecurity strategy for the nation. The directives and initiatives created include the 2003 *National Strategy to Secure Cyberspace*, 2003 Homeland Security Presidential Directive 7 (HSPD-7), 2008 Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), and President Obama's 2009 Cyber Policy Review. Conversely, both branches have struggled in providing a comprehensive strategy germane to the current cyber environment. A strategic handicap caused by the rigid nature of a bureaucratic system that does not adapt very well to the rapidly changing environment of the cyber domain.

Initiated by the Bush administration, *The National Strategy to Secure Cyberspace* initially recognized that securing cyberspace was a global matter due to its interconnection with information systems around the world. The directive stated that securing global cyberspace would require international cooperation to raise awareness, increase information sharing, promote security standards, and investigate and prosecute those who engage in cybercrime.³³ In addition, the strategy identifies the lead agencies and their respective cybersecurity sectors. For example, Department of the Treasury is responsible for the Banking and Finance sector, and Department of Defense is responsible for the Defense Industrial Base sector.

Augmenting *The National Strategy to Secure Cyberspace*, the Homeland Security Presidential Directive 7 identified the roles of federal, state, and local agencies protecting critical

infrastructures from terrorist attacks. The directive provided policies regarding cybersecurity and directed the Department of Homeland Security (DHS) to develop a comprehensive and integrated plan to outline goals and key initiatives to protect critical infrastructure and key resources. It further stated that the Department of State would work in conjunction with Department of Justice, Commerce, Defense, the Treasury and other appropriate agencies, to work with international organizations and foreign countries to strengthen the protection of United States critical infrastructure and key resources.

The Comprehensive National Cybersecurity Initiative, established by National Security Presidential Directive 54/Homeland Security Presidential Directive 23, focused on safeguarding federal executive branch government information systems, it includes one initiative focused on building an approach that deters interference and attacks in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors.³⁴ This initiative focused primarily on the security of Executive Branch networks.

President Obama's *Cyberspace Policy Review* was a 60-day evaluation that assessed the state of the nation's cyber defenses. Fundamentally, the review was an "administrative plan" to initiate a "comprehensive plan" for cybersecurity. The plan builds on the 2008 *Comprehensive National Cybersecurity Initiative* and encourages transparency in order to allow individuals, academia, industry, and governments to engage.

Although the federal government has made efforts in developing cyberspace governance and security, these policies and initiatives are limited in delivering an effective national cybersecurity strategy. For instance, while the 2003 *National Strategy to Secure Cyberspace* declares Department of Homeland Security as lead for all federal agencies, the strategy does not provide

any objectives or time frames required to satisfy the national strategy. Likewise, President Obama's *Cyberspace Policy Review* states that a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation will be built in the near-term; however, it does not provide information on time frames or supporting activities in which to fulfill this or other objectives listed. The doctrine must articulate and better define agency roles and responsibilities. The Departments of Defense, Commerce, Intelligence Community, Homeland Security, and other government affiliations have various overlapping and potentially competing responsibilities. Even though initiatives are being carefully crafted at the agency level, the executive branch must develop an overarching cybersecurity strategy that will ensure unity of effort. This will eliminate the possibility of agencies overstepping their boundaries and creating friction between the government entities. Furthermore, the cybersecurity doctrine must be coherent and have continuity with other supplemental documents in terms of policies and strategies. A national strategy would set clear desired results and priorities, specific milestones, and outcome-related performance measures while giving implementing parties flexibility to pursue and achieve those results within a reasonable timeframe.³⁵ These specifications can be accomplished by employing the OODA Loop decision-making concept. Its ability to adapt to a continuously changing environment allows the OODA Loop to formulate strategies germane to the problems in the Information Age. In addition, the feedback-linked cyclic process leverages the information distributed across the organizational echelons. As a result, there is a unity of effort from all organizations and the intent of the cybersecurity strategy is understood by all.

Conclusion

The United States faces some unprecedented challenges ahead in the Information Age. Unfortunately, cybersecurity was not taken into consideration during the development of the United States federal government or cyberspace. Created during the Industrial Age, the network was physically protected under lock and key within a facility. Today, the network remains fragile and unsecure, only retrofitted with security components. With the current legacy framework in place, it is doubtful that the United States can completely secure itself from pervasive cyber confrontation.

The Cybersecurity Strategy Formulation Model allows policymakers and defenders to orient themselves to the cyber environment by understanding the cyber domain, the attacker, and the motives and goals of an attacker. The integration of Boyd's OODA Loop provides the Cybersecurity Strategy Formulation Model the ability to adapt to the pervasively and rapidly evolving cyber threat. However, there must be a multidisciplinary effort provided by international authorities. Cyber attacks are not geographically restricted to a certain area and possess the aptitude to span across the globe. Hence, each phase of protection must involve the interaction of private-public sectors and international governments. This interaction allows there to be consensus among the international community and stakeholders involved in creating and identifying the intent of the global strategy. Moreover, this effort would mitigate the disparity among the laws of nations, modernize the laws for cybersecurity and increase the technical proficiency of the legislative systems. Unifying efforts between international cyber coalitions will allow the United States to protect vulnerable information critical to national security.

Bibliography

Alberts, David S. and Hayes, Richard E. *Power to the Edge: Command...Control...in the Information Age*. Washington, D.C.: Department of Defense, 2005.

Boyd, John R and Spinney, Chuck, ed. *Patterns of Conflict*. Atlanta: Defense and the National Interest, 1986.

Capehart, Barney L. and Capehart, Lynne C., ed. *Web Based Enterprise Energy and Building Automation Systems*. Lilburn, GA: The Fairmont Press, Inc., 2007.

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol: O'Reilly Media, Inc., 2010.

Clarke, Richard A. and Knake, Robert K. *Cyber War*. New York: HarperCollins Publishers, 2010.

Clausewitz, Carl Von, Howard, Michael, ed and Paret, Peter, ed. *On War*. New Jersey: Princeton University Press, 1984.

Coram, Robert. Boyd: *The Fighter Pilot Who Changed the Art of War*. New York: Back Bay Books, 2002.

Cyber-Attack. New York: Oxford University Press Inc, 2003.

Department of Homeland Security. *Cyber Storm Exercise Report*. September 12, 2006.

Gallagher, Michael P., Link, Albert N. and Rowe, Brent R. *Cyber Security: Economic Strategies and Public Policy Alternatives*. Northampton: Edward Elgar Publishing, Inc., 2008.

Halpin, Edward, Trevorrow, Webb, David and Wright, Steve. *Cyberwar, Netwar and the Revolution in Military Affairs*. New York: Palgrave Macmillan, 2006.

Huntley, Todd C. Huntley. "Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Naval Law Review. Conflict During a Time of Fundamental Change in the Nature of Warfare." *Naval Law Review*. 2010.

Janczewski, Lech J. and Colarik, Andrew M. *Cyber Warfare and Cyber Terrorism*. New York: Information Science Reference, 2008.

Joint Chiefs of Staff, *Joint Publication 6-0, Joint Communication System*. June 10, 2010.

Kramer, Franklin D. *Holistic Approaches to Cybersecurity Enabling Network-Centric Operations*. Washington: U.S. Government Printing Office, 2009.

Landler, Mark and Markoff, John. "Digital Fears Emerge after Data Siege in Estonia." *The New York Times*. May 29, 2007.

<http://www.nytimes.com/2007/05/29/technology/29estonia.html> (accessed December 1, 2010).

Latham, Robert, ed. *Bombs and Bandwidth*. New York: The New Press, 2003.

United States Government Accountability Office, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*. July 2010.

Lukasik, Stephen J., Goodman, Seymour E. and Longhurst, David W. *Protecting Critical Infrastructures Against Cyber-Attack*. New York: Oxford University Press Inc, 2003.

National Intelligence Council. *Global Trends 2025: A Transformed World*. November 2008.

http://www.dni.gov/nic/PDF_2025/2025_Global_Trends_Final_Report.pdf (accessed December 1, 2010).

Olsen, Kelly. "Massive Cyber Attack Knocked Out Government Web Sites Starting On July 4." *The Huffington Post*, July 8, 2009.

http://www.huffingtonpost.com/2009/07/07/massive-cyber-attack-knoc_n_227483.html (accessed December 1, 2010).

Ridge, Tom. CACI-United States Naval Institute symposium comments.

Shachtman., Noah. "Under Worm Assault, Military Bans Disks, USB Drives." *Wired*. November 19, 2008. <http://www.wired.com/dangerroom/2008/11/army-bans-usb-d/> (accessed December 1, 2010).

Stiennon, Richard. *Surviving Cyber War*. Lanham: Government Institutes, 2010.

The Economist. Cyberwar: War in the Fifth Domain. *The Economist*. July 1, 2010. <http://www.economist.com/node/16478792/print> (accessed December 1, 2010).

The Sydney Morning Herald. "Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber-Attacks." *The Sydney Morning Herald*. May 16, 2007.

<http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html> (accessed December 1, 2010).

The White House. *The Comprehensive National Cybersecurity Initiative*. Washington, D.C. January 2008.

The White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. May 29, 2009.

The White House. *National Security Presidential Directive 54/Homeland Security Presidential Directive 23*. Washington D.C., January 8, 2008.

The White House. *The National Strategy to Secure Cyberspace*. February 2003.

United States General Accounting Office. *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*. GAO-04-408T. Washington. February 3, 2004.

Notes

- ¹ Joint Chiefs of Staff, *Joint Publication 6-0, Joint Communication System* (June 10, 2010), I-6.
- ² National Intelligence Council, *Global Trends 2025: A Transformed World* (November 2008), 97, http://www.dni.gov/nic/PDF_2025/2025_Global_Trends_Final_Report.pdf
- ³ Robert Latham, ed., *Bombs and Bandwidth* (New York: The New Press, 2003), 7.
- ⁴ The Economist, "Cyberwar: War in the Fifth Domain," *The Economist*, July 1, 2010, <http://www.economist.com/node/16478792/print>.
- ⁵ The White House, *The National Strategy to Secure Cyberspace*, February 2003, 51.
- ⁶ Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Back Bay Books, 2002), 341.
- ⁷ Stephen J. Lukasik, Seymour E. Goodman and David W. Longhurst, *Protecting Critical Infrastructures Against Cyber-Attack* (New York: Oxford University Press Inc, 2003), 11.
- ⁸ Robert Latham, ed., *Bombs and Bandwidth* (New York: The New Press, 2003), 31.
- ⁹ Kelly Olsen, Massive Cyber Attack Knocked Out Government Web Sites Starting On July 4, *The Huffington Post*, July 8, 2009, http://www.huffingtonpost.com/2009/07/07/massive-cyber-attack-knoc_n_227483.html.
- ¹⁰ Stephen J. Lukasik, Seymour E. Goodman and David W. Longhurst, *Protecting Critical Infrastructures Against Cyber-Attack* (New York: Oxford University Press Inc, 2003), 9.
- ¹¹ Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: HarperCollins Publishers, 2010), 289-290.
- ¹² Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol: O'Reilly Media, Inc., 2010), 137.
- ¹³ Barney L. Capehart and Lynne C. Capehart, ed., *Web Based Enterprise Energy and Building Automation Systems* (Lilburn, GA: The Fairmont Press, Inc., 2007), 357.
- ¹⁴ Select Comm. on Holistic Approaches to Cybersecurity Enabling Network-Centric Operations, H.A.S.C. No. 110-141, pt. 2 (2008).
- ¹⁵ John R. Boyd, *Patterns of Conflict*, 70.
- ¹⁶ Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Back Bay Books, 2002), 335.

- ¹⁷ Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (New York: Routledge, 2007), 227.
- ¹⁸ Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Back Bay Books, 2002), 336.
- ¹⁹ *Ibid.*, 335.
- ²⁰ Alvin Toffler, *War and Anti-War* (Boston: Warner Books, 1995).
- ²¹ David S. Alberts and Richard E. Hayes, *Power to the Edge: Command...Control...in the Information Age* (CCRP, 2005), 203.
- ²² "Estonia urges firm EU, NATO response to new form of warfare: cyber-attacks", The Sydney Morning Herald, May 16, 2007, <http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html>.
- ²³ *Ibid.*
- ²⁴ Mark Landler and John Markoff, "Digital Fears Emerge after Data Siege in Estonia", *The New York Times*, May 29, 2007, <http://www.nytimes.com/2007/05/29/technology/29estonia.html>.
- ²⁵ *Ibid.*
- ²⁶ Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: HarperCollins Publishers, 2010), 20.
- ²⁷ Department of Homeland Security, *Cyber Storm Exercise Report* (September 12, 2006), 3.
- ²⁸ A. Clarke and Robert K. Knake, *Cyber War* (New York: HarperCollins Publishers, 2010), 25.
- ²⁹ Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol: O'Reilly Media, Inc., 2010), 137.
- ³⁰ Noah Shachtman, Under Worm Assault, Military Bans Disks, USB Drives, *Wired*, November 19, 2008, <http://www.wired.com/dangerroom/2008/11/army-bans-usb-d/>
- ³¹ Todd C. Huntley, "Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review* (2010), 2.
- ³² The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 29, 2009), iv.

³³ The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C., February 2003), 51.

³⁴ The White House, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* (Washington D.C., January 8, 2008).

³⁵ United States General Accounting Office, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, February 3, 2004), 16.